Order Code RL31542

Report for Congress

Homeland Security – Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview

Updated December 12, 2002

Jeffrey W. Seifert
Analyst in Information Science and Technology Policy
Resources, Science, and Industry Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
12 DEC 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Homeland Security Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service The Library of Congress 101 Independence Ave. SE Washington, DC 20540**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**26**	

Homeland Security – Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview

Summary

This report assesses the impact of the September 11, 2001 attacks on public and private information infrastructures in the context of critical infrastructure protection, continuity of operations (COOP) planning, and homeland security. Analysis of the effects of the terrorist attacks suggests various "lessons learned." These lessons support three general principles. The first principle emphasizes the establishment and practice of comprehensive continuity and recovery plans. One lesson learned in this area is to *augment disaster recovery plans*. Businesses and agencies, who now must consider the possibility of complete destruction and loss of a building, may need to augment their disaster recovery plans to include the movement of people, the rapid acquisition of equipment and furniture, network connectivity, adequate workspace, and more. A corollary to this lesson learned is the need to assure that recovery procedures are well documented and safeguarded so that they can be fully utilized when necessary. A second lesson is the need to *back up data* ***and*** *applications*. Without a comprehensive backup system that captures more than just an organization's data files, a significant amount of time can be lost trying to re-create applications, organize data, and reestablish user access. A corollary to this lesson learned is the need to fully and regularly test backup sites and media to ensure their reliability and functionality.

The second principle focuses on the decentralization of operations and the effectiveness of distributed communications. The lesson of *decentralizing operations* can be applied to the structure and location of an organization's operations. Industry experts suggest recovery sites be located at least 20-50 miles away form the primary work site. In addition, some observers suggest that human resources should also be located in more than one place to reduce the potential for losing a significant portion of one's workforce in a single event. Another lesson in this area is to *ensure the ability to communicate with internal and external constituencies*. In the event of an emergency, the demand for information skyrockets. An organization not only needs to communicate with employees regarding actions and procedures, but also with the citizens and customers to whom it is responsible for providing goods and services.

The third principle involves the institutionalization of system redundancies to eliminate single points of weakness. In this context, the lesson of *employing redundant service providers* is applied primarily to telecommunications services. In the event a central switching station is disabled, having multiple providers using different infrastructures for access can reduce the possibility of an organization losing its communications services and being unable to carry out its responsibilities. Another related lesson learned is the *use of generic replaceable technology*. In the event of a catastrophe, the ability to replace equipment quickly with easy-to-find products that do not require comprehensive customization, can contribute significantly to how quickly an organization's operations can be functional again. This report will be updated as events recommend.

Contents

Homeland Security – Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview

Introduction

Analysis of the effects of the terrorist attacks of September 11, 2001, suggests various "lessons learned" concerning public and private information infrastructures. What results are some insights to the range of challenges and opportunities facing policymakers as they seek to identify relevant technical solutions to homeland security concerns. This report considers these homeland security issues in the context of critical information infrastructure protection and continuity of operations (COOP) planning.

As part of the congressional and presidential efforts to develop and implement a comprehensive homeland security strategy and establish a Department of Homeland Security, the role of information technology (IT) has become an increasingly important focus. In Congress, bills have been introduced and are being actively considered in both the House of Representatives[1] and the Senate[2] regarding the establishment of a new department dedicated to homeland security issues.[3] Although they differ on the details, the bills include provisions regarding the proposed department's organizational composition, administrative structure, and functional responsibilities. In July 2002, the President released the country's first *National Strategy for Homeland Security*, outlining the strategic objectives, critical mission areas, and initiatives in support of the Administration's proposed Department of Homeland Security.[4] The strategic objectives include: prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism; and minimize the

---

[1]H.R. 5005, Homeland Security Act of 2002, has served as the primary legislative proposal being considered in the House of Representatives regarding the creation of a new Department of Homeland Security. H.R. 4660, National Homeland Security and Combating Terrorism Act of 2002 is the House counterpart to S. 2452.

[2]S. 2452, National Homeland Security and Combating Terrorism Act of 2002, has served as the primary legislative proposal being considered in the Senate regarding the creation of a new Department of Homeland Security.

[3]For a detailed analysis of the proposals to create a new Department of Homeland Security, see CRS Report RL31513 *Homeland Security: Side-by-Side Comparison of H.R. 5005 and S. 2452, 107th Congress*, by the CRS Homeland Security Team, and CRS Report RL31493 *Homeland Security: Department Organization and Management*, by Harold C. Relyea.

[4]See [http://www.whitehouse.gov/homeland/book/index.html].

damage and recover from attacks that do occur. Common to both the national strategy document and the proposed legislation is an emphasis on developing information sharing initiatives and fostering partnerships between and within the levels of government and the sectors of industry.

The heavy reliance upon information technology to carry out mission critical tasks and provide other citizen services highlights the need to ensure these assets are protected, backed up, and resilient to attack. Moreover, the growth of the use of electronic government (e-government) applications to conduct government-to-citizen interactions, as well as government-to-business and government-to-government transactions, has put additional pressure on the need to reconstitute systems quickly to minimize any disruptions and financial costs associated with a major infrastructure failure.[5] In addition, renewed emphasis is being placed on reducing the vulnerability of the nation's critical information infrastructures while more fully integrating and utilizing public and private information technology assets.[6] Taken together, these issues demonstrate the importance of ensuring the reliability and continuity of information technology systems, as part of the government's overall approach to homeland security. The accounts of successes and failures regarding how agencies and businesses responded to the September 11, 2001 attacks provide an unusual opportunity to examine options for further improving the nation's emergency preparedness.

Relevance and Context of the September 11, 2001 Attacks

In addition to the destruction of buildings and the loss of life, the September 11, 2001 attacks on the World Trade Center (WTC) and the Pentagon inflicted heavy damage on elements of the country's information and communication infrastructure. This, in turn, affected how both public and private organizations were able to respond to the events of the day. First responders experienced difficulties communicating among themselves.[7] Citizens and some governmental officials experienced problems communicating by telephone due to overloaded and destroyed circuits. As described in the sections below, some agencies and businesses directly affected by the attacks had difficulties recovering and reestablishing data operations due to inadequate infrastructure and/or the lack of backup systems. Faced with an overloaded telecommunications system, many turned to the Internet, which continued to function as designed, to send and receive e-mail messages regarding the safety of family, friends, and colleagues. However, even in areas not directly affected by the attacks, citizens and government employees sometimes found a dearth of information because some agencies shut down Web sites or did not use them to provide information regarding available resources and instructions on when and where to report for work.

---

[5]Paula Musich, "Recovery Service Fetches Mission-Critical Software," *eWeek*, 13 May 2002, p. 21.

[6]For a detailed analysis of critical infrastructure issues, see CRS Report RL30153 *Critical Infrastructures: Background, Policy, and Implementation*, by John Dimitri Moteff.

[7]Michael Powell, "N.Y. Rescuers Disorganized in 9/11 Attack," *Washington Post*, 20 August 2002, A1; McKinsey & Company, *Improving NYPD Emergency Preparedness and Response*, 19 August 2002, p. 26; McKinsey & Company, *Improving FDNY's Preparedness*, 19 August 2002, p. 85.

For example, it was reported that as of nearly 48 hours after they occurred, neither the General Services Administration (GSA) or the Central Intelligence Agency (CIA) had posted any information regarding the terrorist attacks. It was also reported that of the Office of Personnel Management (OPM) shut down its Web site due to concerns related to cyberterrorism.[8]

It is important to note that many of the technology-related problems that emerged from the September attacks have less to do with the capabilities of the technology itself than with how it was implemented. For example, phone lines can be disrupted, so organizations with critical functions need to secure redundant, but separate, means to communicate. Data can be stored and sent nearly anywhere, but agencies need to establish protocols for regularly backing up important information to secure, remote centers. The mixed performance of information infrastructures suggests that both the public and private sectors need to reexamine their information planning and practices so that they can better weather and rebound from catastrophic events. The damage sustained by two important economic and military locations, combined with ongoing efforts to restore services and prepare contingency plans, also raise questions regarding the federal government's role and the private sector's ability to ensure the protection and continuity of the country's information infrastructure (e.g., telecommunications, computer networks, Internet, etc.) in the future.

Nearly a year after the attacks, many organizations are still evaluating the strengths and weaknesses of their information technology resources in the face of such unusual circumstances. It is likely that the full extent of the damage to information technology resources will not be made public due to concerns about national security and business continuity. Traditionally, both public and private sector organizations have been very reluctant to reveal publicly the extent to which their operations are affected by computer viruses and worms, hacker attacks, or similar security weaknesses. This reluctance to share information occurs for two primary reasons. The first is the interest in maintaining the confidence of customers/constituents, and, by extension, in the case of publicly traded companies, maintaining market value. The second reason is concern over being identified as a target for future attacks, and the possibility of revealing (unwittingly or not) other vulnerabilities. However, despite the validity of these concerns, the reluctance to share information with the appropriate actors can serve as an impediment to recovery and prevention planning by further embedding potential weaknesses into the information infrastructure the country has become increasingly dependent upon. Despite the imperfect nature of the information available, a number of lessons learned can be identified and are discussed below. To place these lessons in context, the next section provides a brief synopsis of how the public and private information infrastructures performed and were affected in the wake of the initial destruction and the immediate reaction by individuals, businesses, and the federal government.

---

[8]Dean, Joshua, "E-gov Fails, Succeeds in Tragedy's Wake," *Government Executive Magazine*, 13 September 2001, [http://www.govexec.com/dailyfed/0901/091301j2.htm]. For more information regarding cyberterrorism, see CRS Report RL30735 *Cyberwarfare*, by Steven A. Hildreth.

Summary of the Events and Impact of September 11, 2001

Overview

Due to the evolving nature of available information, it is not possible to provide a comprehensive accounting of all the organizations affected by the terrorist attacks. However, a variety of examples are discussed in context to provide a sense of the range of issues facing the public and private sectors as they seek to implement new initiatives. One means to gain an overall sense of the immediate impact of the September 11, 2001 attacks is to consider how people and organizations communicated.

The attacks spurred a tremendous spike in telephone calls that overloaded the capacity of some networks. Verizon normally handles 115 million calls per day in New York City and 35 million in Washington, DC, for a normal daily total of 150 million calls. Following the attacks, the combined total jumped to 340 million calls. Similarly, Cingular Wireless said its call volume jumped 400%. Requests were made to international telecommunications carriers, such as France Telecom, to control the flow of calls to the United States in an effort to keep trans-Atlantic links open.[9]

Many people turned to cellphone-based text messaging, Internet-based instant messaging, and the use of two-way radio features of cellphones to get around the congested phone networks. AOL reported a 20% jump in instant messaging volume, handling 1.2 billion messages on September 11, 2001.[10]

The National Communications System (NCS) activated the Government Emergency Telecommunications Service (GETS). Using a special phone number and a personal identification number, GETS calls receive priority handling before all other calls on phone lines operated by ATT, Sprint, and WorldCom. During the week following the attacks, 3,000 GETS calls were made in Washington. An additional 4,000 GETS calls to and from Manhattan were completed with a 95% success rate.[11]

The General Services Administration (GSA) also provided mobile communications centers that supported several agencies, including the Federal Bureau of Investigation (FBI). In addition, the GSA Federal Technology Service

---

[9] Joshua Dean, "Looking for Lifelines," *Government Executive Magazine*, 1 October 2001, [http://www.govexec.com/features/1001/1001spec4.htm].

[10] Alex Daniels and Brendan Barrett, "Saved by Text Messages," *Washington Techway*, 1 October 2001, p.14.

[11] Joshua Dean, "Looking for Lifelines," *Government Executive Magazine*, 1 October 2001, [http://www.govexec.com/features/1001/1001spec4.htm].

(FTS) made 500 computers available to agencies within the first two days of the attacks.[12]

Many agencies used their Web sites to keep the public informed and provide information on how to help the victims. One of those was the Federal Emergency Management Agency (FEMA) Web site. FEMA was one of the first agencies to post information about the attacks on the morning of September 11, 2001. On September 12, the FEMA site had 3.4 million visitors, an all-time high for the agency. GSA used its site to notify people about the status of various governmental buildings. Many agencies, including the Department of Defense, used their sites to keep employees informed of changes.[13] Some Members of Congress, including Senators Charles Schumer and Hillary Rodham Clinton of New York, and Senator George Allen of Virginia, also turned their congressional sites into information centers regarding the attacks.[14]

FirstGov's Web staff, who were evacuated from their Washington, DC, offices, worked at home immediately following the attacks, collecting information, phone numbers, and URLs for relevant sites. They posted this information to the FirstGov site on September 12. Many commercial news sites and other government sites then posted links to the FirstGov site[15], helping drive 448,552 unique visitors accounting for 1.75 million page hits during the week of September 9-15. FirstGov also changed its site update schedule from every two weeks to updating it every 12 hours.[16]

New York - the World Trade Center

At 8:45 AM, American Airlines Flight 11 crashed into the north tower of the World Trade Center. Eighteen minutes later, United Airlines Flight 175 crashed into the south tower. The eventual collapse of both towers inflicted heavy damage to the surrounding buildings and infrastructure, ultimately resulting in the collapse of other buildings on the site and the deaths of nearly 3,000 people. The attacks displaced large numbers of both public and private sector employees. The World Trade Center contained an estimated 430 tenants with 50,000 employees (not all present at the time of the attack), and typically received another 140,000 visitors on a daily basis.[17]

---

[12]Timothy B. Clark, Shane Harris, and Tanya N. Ballard, "GSA Chief Praises Employees for Reaction to Attacks," *Government Executive Magazine*, 20 September 2001, [http://www.govexec.com/news/index.cfm?mode=report&articleid=21133].

[13]Christopher J. Dorobek, Christopher J., "Web Sites that Worked," *Federal Computer Week*, 1 October 2001, p.18.

[14]Patrick Smith, "Agency Webmasters Aid in Recovery," *Government Computer News*, 8 October 2001, p.16.

[15]FirstGov is a portal site administered by the General Services Administration (GSA) that is designed to serve as "the official U.S. gateway to all government information." The FirstGov site is located at: [http://www.firstgov.gov].

[16]Patricia Daukantas, Patricia, "FirstGov Handles Millions of Web Hits After Attacks," *Government Computer News*, 8 October 2001, p.1.

[17]"List of World Trade Center Tenants," *CNN.com*, September 2001, (continued...)

According to the General Services Administration (GSA), more than 2,800 federal employees worked in offices leased by the GSA in Buildings 6 and 7 of the World Trade Center complex. Building 6 had over 2,000 federal employees from a variety of agencies, including the Customs Service, Bureau of Alcohol, Tobacco, and Firearms (ATF), the Occupational Safety and Health Administration (OSHA), the Export-Import Bank, the Foreign Commercial Service of the Department of Commerce, and the Pension and Welfare Benefits Administration of the Labor Department.[18] Among the tenants of Building 7 were 760 federal employees from agencies including the Secret Service, the Equal Employment Opportunity Commission (EEOC), the Department of Defense, and the Internal Revenue Service (IRS).[19] Another 25,000 federal employees were evacuated from four nearby buildings; 26 Federal Plaza, 290 Broadway, 40 Centre Street, and 500 Pearl Street.[20]

The attacks also inflicted heavy damage on elements of the city's information and communication infrastructure, including both land lines and wireless services. One switching facility, which handled 40% of the lower Manhattan phone lines and 20% of the New York Stock Exchange's (NYSE) traffic, was damaged when steel beams from a collapsing building punctured the switching station, flooding it with water and debris. A second switching facility, which normally handles 80% of the NYSE's 15,000 phone and data lines, did not suffer direct damage, but was rendered inoperable by intermittent power outages.[21] In addition, several wireless cell sites were destroyed and others were rendered inactive by power outages. Communication between the New York Fire Department, the Emergency Medical Systems (EMS), and the New York Police Department were also cut off due to the loss of an antenna that had been on 1 World Trade Center.[22] By January 2002, Verizon had restored service to 99% of the affected area.[23]

Local television stations were also affected. Nearly all of the broadcasters had their main antennas located on the roof of the north tower of the World Trade Center.

---

[17](...continued)
[http://www.cnn.com/SPECIALS/2001/trade.center/tenants1.html].

[18]Tanya N. Ballard, Tanya N., "Horror, Then A Helping Hand," *Government Executive Magazine*, 1 October 2001, [http://www.govexec.com/features/1001/1001spec2.htm].

[19]Tanya N. Ballard and Jason Peckenpaugh, "New York Agencies Regroup After Loss of Offices," *Government Executive Magazine*, 12 September 2001, [http://www.govexec.com/dailyfed/0901/091201p2.htm].

[20]Tanya N. Ballard, Tanya N., "Horror, Then A Helping Hand," *Government Executive Magazine*, 1 October 2001, [http://www.govexec.com/features/1001/1001spec2.htm].

[21]The NYSE resumed trading on September 17, 2001. Gretchen Morgenson, "Wall St. Reopens Six Days After Shutdown," *New York Times*, 18 September 2001, p. A1.

[22]Jayson Blair, "Phone Providers Near Ground Zero are Still Frantically Scrambling to Catch Up," *New York Times*, 8 October 2001, p.B13; Becky Orfinger, "Lessons Learned from the World Trade Center Attack," *DisasterRelief.org*, 16 November 2001, [http://www.disasterrelief.org/Disasters/011115wtclessons/]; John Rendleman, "Back Online," *InformationWeek*, 29 October 2001, p. 35.

[23]Eric Lipton, "Cleanup's Pace Outstrips Plans for Attack Site," *New York Times*, 7 January 2002, [http://www.nytimes.com/2002/01/07/nyregion/07SITE.html].

Two stations had backup antennas on the Empire State Building, allowing their signals to still be received by most citizens who were not wired for cable television. The other broadcasters had to utilize towers in more distant locations, such as Alpine, NJ, where they could only reach portions of the New York metropolitan area. As of late June 2002, broadcasters were continuing to work with lawmakers to try to identify a new site for a common tower that would be located within the 3.2 mile radius of the World Trade Center site, necessary to reach the local residents while not interfering with broadcasts in Philadelphia or Boston.[24]

Virginia - the Pentagon

At 9:38 AM, American Airlines Flight 77 crashed into the west face of the Pentagon, killing 64 passengers on board and 125 additional people on the ground. The crash and ensuing fire destroyed an estimated 10% of the Pentagon's office space, and reportedly disrupted one of the Pentagon's two major communications lines.[25] The Navy lost 70% of its Pentagon offices, including a portion of the Navy's budget office, the Office of the Chief of Naval Operations, and its telecommunications operation center.[26] The U.S. Army's Information Management Support Center also received significant damage, losing most of its desktop computers, its entire central help desk, and apparently was unable to access its backup tapes.[27] In addition, the Defense Finance and Accounting Service was damaged. *Computerworld* magazine suggested that many of the Navy's top-secret network operations were probably damaged, although it was believed to be unlikely that this affected the Navy's ability to communicate sensitive information to Navy vessels.[28]

The attack on the Pentagon caused the loss of knowledge assets, including hard copies and data on workstations and servers that were not duplicated or backed up

---

[24]Jayson Blair, "Lawmakers Seeking Site for Antenna in New York," *New York Times*, 29 June 2002, B2; Jayson Blair, "After an Antenna Tumbles, Cable Firms Gain Thousands of New Customers," *New York Times*, 3 March 2002, A35; Raymond Hernandez, "U.S. Providing $8.2 Million to Rebuild TV Antennas," *New York Times*, 23 December 2001, A38.

[25]Input, "Attack on America: The Impact of the September 11 Terrorist Attacks on the Federal Government," 3 October 2001, [http://www.inputgov.com/index.cfm?page=include_article.cfm&article_id=310]; George I. Seffers, "Report Logs Fed IT Losses," *Federal Computer Week*, 1 October 2001, [http://www.fcw.com/fcw/articles/2001/1001/web-input10-01-01.asp].

[26]Dawn S. Onley, "Navy Staff Moves Out While Pentagon Rebuilds," *Government Computer News*, 8 October 2001, p.34; Dan Verton, "IT Operations Damaged in Pentagon Attack; Equipment on Emergency Order," *Computerworld*, 24 September 2001, p.13.

[27]Dawn S. Onley, "A Support Team's Extreme Test,"*Government Computer News*, 3 June 2002, p. 32.

[28]Dan Verton, "IT Operations Damaged in Pentagon Attack; Equipment on Emergency Order," *Computerworld*, 24 September 2001, p.13.

and stored in a different physical location, according to media reports.[29] It is not clear how much information may have been permanently lost or to what degree a lack of backed up information hampered efforts to continue the operations of the affected offices. One office that was able to resume its functions quickly was the Defense Finance and Accounting Office, which maintains servers located in Ohio.[30] Also, the Navy was able to utilize its recently signed Navy Marine Corp Intranet (NMCI) contract to assist its efforts to resume operations. Using the NMCI contract, the Navy relocated approximately 1,000 of its displaced personnel to temporary offices in Arlington, VA, and had 860 laptop computers, 335 desktop computers, and 30 servers, routers, and cabling delivered and installed in just over one week. The Navy's Budget Office, which was in the middle of preparing its budget that was due October 6 when the attacks occurred, lost part of its server farm. However, it had 50 computers and its server farm restored by Sunday, September 16.[31] Efforts to reconstruct and repair the 400,000 square feet of damaged Pentagon offices, dubbed Project Phoenix, have progressed rapidly, with the first group of people moving back into their rebuilt offices on August 15, 2002.[32]

Lessons Learned

In the months following September 11, 2001, there have been a number of accounts of successes, failures, and 'lessons learned' regarding continuity and disaster recovery planning. In many cases, these descriptions are specific to a particular organization or business activity. However, one can identify some observations and lessons learned that are widely applicable and that policymakers and business leaders may wish to consider as they develop and implement new homeland security initiatives.

Continuity of operations (COOP) and disaster recovery planning are not new concepts. However, surveys have shown that only about half of American businesses have disaster management plans in place. In many cases, past threats are often the motivating influences for organizations to make these plans. For example, Morgan Stanley, one of the tenants in the south tower of the World Trade Center, adopted thorough plans in response to bomb threats being made during the Persian Gulf War

---

[29]Input, "Attack on America: The Impact of the September 11 Terrorist Attacks on the Federal Government," 3 October 2001, [http://www.inputgov.com/index.cfm?page=include_article.cfm&article_id=310]

[30]Input, "Attack on America: The Impact of the September 11 Terrorist Attacks on the Federal Government," 3 October 2001, [http://www.inputgov.com/index.cfm?page=include_article.cfm&article_id=310]

[31]Paula Musich, "Navy Turns to EDS, NMCI for Help," *eWeek*, 29 October 2001, p.28; Dawn S. Onley, "Navy Staff Moves Out While Pentagon Rebuilds," *Government Computer News*, 8 October 2001, p.34; Dawn S. Onley, "Navy Reboots Quickly After Sept. 11," 5 November 2001, *Government Computer News*, p.36.

[32]Steve Vogel, "Retaking a Lost Position," *Washington Post*, 16 August 2002, p. A1; Walker Lee Evey, "Pentagon Renovation and Rebuilding Briefing," *DefenseLINK*, 7 March 2002, [http://www.defenselink.mil/news/Mar2002/t03072002_t0307pen.html].

in 1991, and reinforced those plans following the 1993 bombing of the World Trade Center. The financial services firm's regular evacuation drills are credited as one of the reasons why nearly all of its approximately 3,500 employees were able to escape before the buildings collapsed.[33]

In the case of information technology disaster recovery planning, preparation for the year 2000 transition (Y2k) has been cited by a number of private and public sector organizations as one of the main reasons they were able to respond and recover quickly from the September 11, 2001, attacks.[34] Y2k planning began substantially in the 1990s, led primarily by the private sector and followed by federal and state government agencies.[35] Y2k preparation spurred many organizations to operationalize strategies for backing up data, enabling remote working, and enhancing communication links between organizations, employees, customers, and vendors.[36] Many tenants of the World Trade Center also cited the 1993 bombing of the building as their rationale for having developed extensive disaster recovery plans, which they, in turn, attributed to their success in evacuating employees and preserving vital data.[37]

The amount of time and resources spent on information technology disaster planning can vary with the size and type of organization. According to the Gartner Group, a research and advisory firm, an average company allocates approximately three percent of its annual information technology budget to disaster recovery. In contrast, financial services companies, which have to meet requirements set by the Federal Reserve Board and/or the Securities and Exchange Commission (SEC), spend an average of seven to eight percent.[38]

However, if it may seem costly to dedicate a significant portion of one's budget to planning for an event with a low chance of occurring, the financial consequences for being unprepared can be even higher. In the case of financial companies, many, if not most, had invested in data backup and disaster recovery facilities to one degree or another. While this allowed them to save a significant amount of customer and business-critical data, it is estimated that these firms will still spend $3-5 billion over

---

[33]James Schulz, "New Urgency for Disaster Recovery Planning," *Washington Technology*, 8 October 2001, p.18; Michael Grunwald, "A Tower of Courage," *Washington Post*, 28 October 2001, p.F01.

[34]Dibya Sarkar, "Crisis Plan, Tech Helped NYC," *Government E-Business*, 14 December 2001, [http://www.fcw.com/geb/articles/2001/1210/web-nyc-12-14-01.asp].

[35]James Schulz, "New Urgency for Disaster Recovery Planning," *Washington Technology*, 8 October 2001, p.18.

[36]Mark Hall, "Managers Find Preparedness Pays Off," *Computerworld*, 17 September 2001, p.1.

[37]Stan Gibson, "Lessons Learned Speed WTC Recovery," *eWeek*, 20 September 2001, [http://zdnet.com.com/2100-1104-504061.html?legacy=zdnn].

[38]Maggie Semilof, "Hackers, Not Terrorists, Major Concern," *InternetWeek*, 1 October 2001, p.11.

the next two years to replace their destroyed information technology infrastructure.[39] For example, Dow Jones Inc., a global financial news company and publisher of *The Wall Street Journal* and Barron's publications, was expected to spend $2 million to replace information technology hardware and office equipment.[40] Although it had relatively few offices in or around the World Trade Center and a portion of the affected area of the Pentagon was not occupied, the federal government will also be spending a significant amount to replace lost and damaged information technology systems. Input, a Web-based information technology market research and marketing services firm, predicted that the federal government will spend $75 million, with the Customs Service alone expected to account for $15 million of that amount.[41]

While information technology disaster recovery planning is often compared to the preparations for Y2k, it is important to recognize that these scenarios are qualitatively different. Y2k had a finite time line with a clear indicator of success or failure. In contrast, the war on terrorism appears to be an open-ended and evolving process. As the examples below demonstrate, measures of success are relative, and the task of planning is never truly done. The lessons learned today can help prepare for tomorrow, but they do not represent the final word on information technology disaster recovery planning.

Lessons Regarding Continuity and Recovery Planning and Practices

The events of September 11, 2001, have brought a new urgency to continuity and recovery planning and practices. While attention has been growing over time, this multifaceted undertaking can often be a very challenging and frustrating process as planners try to coordinate disparate parts of their organizations while trying to strike a balance between how much they *cannot* afford to be unprepared and how much they can afford to spend on resources they may never use. Further complicating matters has been the tendency for organizations to "stovepipe" the different protections relevant to information technology disaster recovery planning. For example, information security has often been handled independently from physical security. Similarly, the compartmentalization of an organization's units and processes can contribute to a fractured planning process that can leave an organization vulnerable.[42]

---

[39]Lucas Mearian, "The Toll on Wall Street," *Computerworld*, 17 September 2002, p.6; Rutrell Yasin, "Financial Firms' Hefty Bill," *InternetWeek*, 22 October 2001, p.7.

[40]Deidre Lanning and Matthew Maier, "The I.T. Toll," *Business 2.0*, December 2001, p.122.

[41]Joshua Dean, "Agencies Likely to Spend Millions on Technology to Recover From Attacks," *Government Executive Magazine*, 28 September 2001, [http://www.govexec.com/dailyfed/0901/092801j1.htm]; Input, "Attack on America: The Impact of the September 11 Terrorist Attacks on the Federal Government," 3 October 2001, [http://www.inputgov.com/index.cfm?page=include_article.cfm&article_id=310].

[42]James Schulz, "New Urgency for Disaster Recovery Planning," *Washington Technology*, 8 October 2001, p.18.

One reported example indicating the possible costs and consequences when an organization does not have a fully integrated plan is the May Davis Group. The privately held financial services company had its offices on the 87th floor of one of the World Trade Center towers. In addition to losing $100,000 of equipment, the firm apparently lost some regulatory documents and $1 million in revenue due to data loss and downtime.[43]

A less severe example is the Secret Service field office, located in 7 World Trade Center, which did have a contingency plan, but had not fully implemented it at the time of the attack. The agency's field office was able to resume operations the following day at an alternative location. It reportedly lost some of the information it was collecting on criminal suspects.[44]

Another example is Deloitte Consulting, whose primary telecommunications hub in New York City, located in the World Financial Center next to the World Trade Center towers, was put out of service, affecting an estimated one thousand employees in the area. As a consulting firm, Deloitte considers its ability to share information with clients to be its core business. During the weeks it took to rebuild its land line communication center, Deloitte's New York area employees used cell phones to stay in contact with customers and fellow employees.[45]

Even organizations that have planned extensively can sometimes overlook small details that appear insignificant, but later prove to be important. One such example is American International Group (AIG) Inc. The financial services company has offices and information technology operations near the World Trade Center site. Using its backup business center in Parsippany, NJ, and a second previously contracted emergency facility in Livingston, NJ, AIG was able to use data from its automated backup system to be operational the day after the attacks. However, not all of its servers were part of the automated backup system, and the backup tapes for these servers reportedly were left behind when its building was evacuated.[46]

Augment Disaster Recovery Plans

In many respects, the September 11, 2001, attacks established a new standard for disaster recovery plans – the complete destruction and loss of a building. Even among some of the most prepared organizations, their plans sometimes presumed the ability to eventually return to their offices, even if only to retrieve equipment and

---

[43]Deidre Lanning and Matthew Maier, "The I.T. Toll," *Business 2.0*, December 2001, p.122; Bill Atkinson, "A Local Firm Rebuilds from Ground Zero," *The Baltimore Sun*, 30 September 2001, 1C.

[44]Matt McLaughlin, "War on Terrorism Speeds Many Federal IT Plans," *Government Computer News*, 19 November 2001, p.7; Tanya N. Ballard and Jason Peckenpaugh, "New York Agencies Regroup After Loss of Offices," *Government Executive Magazine*, 12 September 2001, [http://www.govexec.com/dailyfed/0901/091201p2.htm].

[45]Eileen Conklin, "Deloitte Won't Get Caught Short," *InformationWeek*, 8 April 2002, p. 49.

[46]Martin J. Garvey, "Bounce Back," *InformationWeek*, 22 October 2001, p.35.

paper files.[47] Modern fire safety and construction methods have largely made the possibility of a building collapse less likely, so many organizations developed plans that focused on the movement of data to be used temporarily at a backup facility. These same businesses and agencies must now consider whether to augment their disaster recovery plans to include the movement of people, the rapid acquisition of equipment and furniture, network connectivity, adequate workspace, and more. Some organizations may need to be able to not just store, but also to run mission critical applications, at their backup sites, and staff may need to be trained to implement such a plan.[48] The possible need for more sophisticated data backup facilities suggests organizations may consider establishing a 'hot site'. A hot site is a facility that has all of the data, equipment, software, connectivity, furniture, and office space assembled and ready to use so that an organization can continue its computer operations uninterrupted in the event of a disaster. In some cases, organizations will mirror their data directly to the hot site as an additional backup or in lieu of using backup tapes at the primary site. While hot sites provide the greatest amount of redundancy and readiness, the cost of establishing and maintaining such a site can cost millions of dollars, with additional yearly maintenance costs.[49] This raises cost effectiveness issues. Some hot sites, however, might serve a dual purpose, such as a secondary data site or as part of a comprehensive backup system.[50]

Organizations with more detailed recovery plans were often able to respond better to the events of September 11, 2001. In the case of the Occupational Safety and Health Administration (OSHA), the 21-member office had a contingency plan for its contingency plan. After evacuating, the OSHA employees discovered their first designated meeting site was inaccessible, so they regrouped at a nearby regional office. After this office was evacuated, they gathered at a third site to implement their plan to provide advice and technical assistance to businesses and agencies in an effort to protect workers from being exposed to hazardous substances and other safety risks at ground zero.[51]

A second example is the New York Board of Trade (NYBOT), which handles trading for commodities such as coffee, sugar, and orange juice. NYBOT had invested in a hot site in Queens, NY, which included limited space for a reduced number of trading pits. According to one report, NYBOT had invested $1.75 million

---

[47]Stan Gibson, "Lessons Learned Speed WTC Recovery," *eWeek*, 20 September 2001, [http://zdnet.com.com/2100-1104-504061.html?legacy=zdnn].

[48]Anne Chen and Matt Hicks, "How to Stay Afloat," *eWeek*, 8 October 2001, p.49; James Schulz, "New Urgency for Disaster Recovery Planning," *Washington Technology*, 8 October 2001, p.18; Dawn S. Onley, "A Support Team's Extreme Test," *Government Computer News*, 3 June 2002, p. 32.

[49]Eileen Colkin, "Keep it Simple," *InformationWeek*, 28 January 2002, p.35.

[50]Martin J. Garvey, "Bounce Back," *InformationWeek*, 22 October 2001, p.35; James Schulz, "New Urgency for Disaster Recovery Planning," *Washington Technology*, 8 October 2001, p.18.

[51]Tanya N. Ballard, "OSHA's New York Employees Work Through the Pain," *Government Executive Magazine*, 6 February 2002,
[http://www.govexec.com/dailyfed/0202/020602t1.htm].

to establish the facility, which cost an additional $300,000 per year to maintain. However, while an extended outage would have resulted in the rapid loss of trading contracts to other exchanges in the United States and abroad, NYBOT's investment paid off, allowing it to resume modified trading operations one day after the attacks.[52]

A corollary to this lesson learned is the need to assure that recovery procedures are well documented and safeguarded . Employees need to be well-informed and practiced for the responsibilities they are expected to carry out. Correspondingly, just as one would not keep the sole backup tapes of important information at the primary data center in which they were created, a prudent step would be to keep one or more copies of the recovery plans available at the appropriate off-site locations.

Backing Up Data *and* Backing Up Applications

A second lesson learned that is related to continuity and disaster planning and practices is the need to have a comprehensive backup system that captures more than just an organization's data files. As discussed above, most of the financial services firms in or near the World Trade Center had comprehensive data management and recovery systems in place. Some highly automated systems will begin backing up data to a remote center when a significant temperature change or power loss in the building is detected.[53] Cantor Fitzgerald, one of the hardest hit financial services companies, losing 733 of its approximately 1,000 World Trade Center employees, including 150 information technology workers, lost none of its data due to a system that mirrored all of its software and data to its data center in Rochelle Park, NJ.[54] In contrast, the U.S. Customs Service was not as well prepared. In addition to experiencing difficulties finding alternative office space for its 800 displaced employees, the office located in the World Trade Center complex did not have all of its files backed up to computers in its Washington, DC, headquarters. Several months after the attack, the Customs Service reportedly was still working to re-create some of its files from scratch while others are considered permanently lost.[55]

In addition to backing up data, organizations also need to backup the data catalogs, directories, and software applications used with the data. Organizations that saved only their raw data had to spend a significant amount of time re-creating their applications, organizing the data, and reestablishing user permissions to access the data.[56] One company that apparently experienced this problem was NYBOT.

---

[52]Eric Chabrow, and Martin J. Garvey, "Playing for Keeps," *InformationWeek*, 26 November 2001, p.39.

[53]Ashlee Vance, "After the Terror, Companies Rethink Some IT Investments," *Computerworld*, 25 September 2001, [http://www.computerworld.com/storyba/0,4125,NAV47_STO64211,00.html].

[54]Stan Gibson, "Rethinking Storage," 15 October 2001, *eWeek*, p.1.

[55]Tanya N. Ballard, "Feds in New York Slowly Recover From Attacks," *Government Executive Magazine*, 29 January 2002, [http://www.govexec.com/dailyfed/0102/012902.htm].

[56]Martin J. Garvey, "A New Game Plan," *InformationWeek*, 29 October 2001, p.22.

Despite its extensive hot site contingency plan, NYBOT lost some financial records, applications, and e-mail files that were not backed up to the site. Some of this information was backed up to tapes, but the tapes were stored in a fireproof safe kept in their World Trade Center tower office.[57]

In addition to taking a broader view of the digital tools and assets to backup and preserve, organizations – such as regulatory agencies and insurance companies – that still rely heavily on paper files may wish to consider digitizing some of their documents as they are received. Despite much touting of the so-called paperless office, the blizzard of paper that accompanied the dust and debris with the collapse of the towers suggests many organizations are still heavily dependent on their physical documents. However, the high cost of digital imaging requires companies and agencies to consider carefully which documents are most critical and often used.

One company that did have a comprehensive digital imaging system in place before September 11, 2001, was Empire Blue Cross Blue Shield. Developed over the past ten years, starting with claims forms, the insurance carrier's optical storage system captures almost all of its paper documents. As a result, the company lost only about two days' worth of paper mail.[58]

One company that decided to accelerate its plans to digitize and automate its paper-based information is Kemper Casualty Company, which had offices on the 35th and 36th floors of One World Trade Center. The Kemper data backup system had all but the previous day's and that morning's data backed up on tape at its headquarters. It was also able to re-create the lost transactions for the missing data. However, according to media reports, Kemper lost thousands of paper documents, including innumerable insurance policy applications. The company had to spend a significant amount of time and resources to re-create the information by going back to customers and Kemper agents.[59]

The Securities and Exchange Commission, whose New York regional office was located in 7 World Trade Center, also did not digitize its paper records. While the regulatory agency did have a significant amount of its data and files backed up electronically, case files that took years to compile, informal notes written down from interviews and analysis, and other documents were lost. Some of these lost records reportedly were part of pending cases, including those related to investigations of insider trading and financial fraud. While the SEC can have parties submit new copies of documents previously provided, and it may be able to obtain some documents from agencies conducting parallel investigations, documents and other evidence from older cases and smaller companies that are not in operation any longer

---

[57]Jaikumar Vijayan, "Sept. 11 Attacks Prompt Decentralization Moves," *Computerworld*, 17 December 2001, [http://www.computerworld.com/storyba/0,4125,NAV47_STO66660,00.html]; Carol Sliwa, "New York Board of Trade Gets Back to Business," *Computerworld*, 24 September 2001.

[58]Stan Gibson, "Rethinking Storage," 15 October 2001, *eWeek*, p.1.

[59]Marianne Kolbasuk McGee, "A Slow-Moving Industry Picks Up Speed," *InformationWeek*, 21 January 2002, p.33.

may be difficult to recover. The loss and reconstruction of the files may slow down the progress of some investigations and possibly result in others being discontinued.[60]

A corollary to the lessons learned regarding comprehensive data storage plans is the need to fully and regularly test backup sites and media. Organizations that rely on 'cold sites' – backup sites that are not always in use and may require the organization to install hardware, software, or load data to become functional – in the event of a disaster, could experience further problems if they discover their tapes are corrupted or equipment does not work. One organization that regularly tested its backup systems and information was NYBOT. The exchange tested its backup site monthly and practiced its recovery plan every 60 days to assure its systems were working and its employees were familiar with the procedures.[61]

Lessons Regarding Decentralization

A second major category of lessons learned concerns the decentralization of operations and the effectiveness of distributed communications. The rise of networked computing and the Internet has provided the opportunity to connect far-flung locations around the country and the world. Many public and private sector organizations have used this technology to reach outward to new markets, deliver new services, and reduce communications costs. However, the lessons learned discussed below suggest there is also a need for organizations to turn this technology inward to reduce the vulnerabilities of internal operations and to strengthen communications links with internal, as well as external, constituencies.

Decentralize Operations

The maxim, 'don't put all of your eggs in one basket,' can be applied to a variety of situations: college applications, job searches, and investment portfolios. It can also be applied to the structure and location of an organization's operations. Although many of the tenants and neighbors of the World Trade Center had backup facilities, some of these facilities were located within a few blocks of their primary location, resulting in the loss, or at least the inaccessibility, of data at both sites when it was needed most. According to some industry experts, recovery sites should be located at least 20-50 miles way from the primary data center. In addition, some observers suggest that human resources should also be located in more than one spot to reduce the potential for losing a significant portion of one's workforce in a single event.[62]

---

[60]David S. Hilzenrath, "SEC Papers Lost in N.Y. Attacks," *Washington Post*, 13 September 2001, p.E3; Reed Abelson, "S.E.C. Needs a New Home, Fast," *New York Times*, 28 September 2001, [http://www.nytimes.com/2001/09/28/business/28SEC.html].

[61]Eric Chabrow, and Martin J. Garvey, "Playing for Keeps," *InformationWeek*, 26 November 2001, p.39.

[62]Maggie Semilof, "Hackers, Not Terrorists, Major Concern," *InternetWeek*, 1 October 2001, p.11.

As was mentioned above, Cantor Fitzgerald lost 733 of its employees, including 150 of its information technology workers. However, despite this devastating loss, the firm was able to continue its operations in part by relying on employees in its other offices to assume some of the responsibilities of its World Trade Center office.[63] Another company that benefitted from decentralization was Blackwood Trading LLC. The brokerage firm's offices were located six blocks from the World Trade Center, part of the area that lost power and communications service, but it mirrored all of its data at a remote site in Jersey City, NJ. It purposely chose a site physically distant from its offices to reduce the chance of a complete loss of data in the event of a terrorist attack or a natural disaster.[64]

Since September 11, 2001, several other firms have decided to heed the decentralization lesson. One of those organizations is Dow Jones. It had maintained offices at One World Financial Center, adjacent to the World Trade Center, which served as a hub for 800 employees and its data production center. While the damage to the building was not significant enough to prevent its eventual repair and reoccupation, the damage did render approximately 100 servers, 400 workstations, and an estimated "millions of dollars" of the company's networking equipment inoperable. As part of its new strategy to reduce its vulnerability, Dow Jones reportedly decided to permanently move the company's data center to its backup facilities in South Brunswick, NJ, and move only half of its employees back to its Manhattan location. The financial information company plans to rely on a network of news and data centers distributed around the country. It will also rely more heavily on remote offices, encourage telecommuting, and establish a new backup facility distant from its South Brunswick data center.[65]

Empire Blue Cross Blue Shield, which benefitted significantly from its extensive backup system, has also decided to decentralize the 1,900 employees from its World Trade Center offices into three different facilities. In addition to spreading the risk, the insurance carrier also observed that it is easier to conduct a data recovery operation for a smaller portion of its operations as compared to the larger whole in the event of a disaster.[66]

Ensure the Ability to Communicate with Internal and External Constituencies

Another lesson learned related to decentralization is the need to ensure the ability to communicate with internal and external constituencies in the event of an emergency. The attacks of September 11, 2001, forced many companies to rely on ad hoc networks to communicate with employees. The overload of telecommunications networks, including cellular voice networks, left many people

---

[63]Stan Gibson, "Dow Jones Leave IT in New Jersey," *eWeek*, 12 November 2001, p.1.

[64]Lucas Mearian, "The Toll on Wall Street," *Computerworld*, 17 September 2001, p.6.

[65]Stan Gibson, "Dow Jones Leave IT in New Jersey," *eWeek*, 12 November 2001, p.1.

[66]Jaikumar Vijayan, "Sept. 11 Attacks Prompt Decentralization Moves," *Computerworld*, 17 December 2001,
[http://www.computerworld.com/storyba/0,4125,NAV47_STO66660,00.html]

scrambling to find a way to get messages out. Some have suggested relying on wireless data backup systems as an alternative to voice networks in the case of an emergency. One such network that proved useful for many people is a data network, which is used to support the BlackBerry pager, a mobile e-mail and paging device.[67] In the weeks following the attacks, the Committee on House Administration supplied BlackBerry devices and monthly service to all 435 Members.[68] Demand for BlackBerry pager devices by other federal agencies has jumped dramatically since September 11, 2001.[69]

Most organizations are aware of the importance of communications with external constituencies: citizens and customers. In the case of government agencies, this function is becoming associated with electronic government. Many people searching for information and guidance during the uncertainty that followed the attacks turned to corporate and agency Web sites. However, the performance of these sites was mixed. Some sites immediately transformed themselves into centers for crisis information, while others were shut down altogether. The Office of Personnel Management (OPM) initially shut down its Web site citing cyber attack concerns. The site was brought back online late in the afternoon of September 11, 2001, with the announcement that agencies in Washington, DC would be open the next day.[70] The Federal Aviation Administration's (FAA) Web site was also offline for a significant portion of the day.[71]

The Department of Defense used its DefenseLink site to provide information and pictures about the attack on the Pentagon. DefenseLink, the Defense Department's main Web site, experienced a 243% increase in page hits the week following the attacks. In order to handle the increased traffic, DoD tripled the sites' bandwidth capacity. Other sites that experienced surges in Web traffic included the FBI, the Department of Justice, and FirstGov.

---

[67]Bob Brewin, and Matt Hamblen, "Alternative Nets Essential in Dealing with Disaster," *Computerworld*, 24 September 2001, p.69.

[68]Ephraim Schwartz, "Congress Going Wireless," *InfoWorld*, 11 October 2001, [http://www.infoworld.com/articles/hn/xml/01/10/11/011011hncongress.xml]; Bob Ney and Steny Hoyer, *All Member Offices to Receive Blackberries*, Dear Colleague Letter, Committee on House Administration, U.S. House of Representatives, 21 September 2001, [http://www.house.gov/cha/publications/DC_s/dc_s.html]; Bob Ney and Steny Hoyer, *BlackBerry Pager Update*, Dear Colleague Letter, Committee on House Administration, U.S. House of Representatives, 16 October 2001, [http://www.house.gov/cha/publications/DC_s/dc_s.html].

[69]Shane Harris, "Agencies Buying Up Field-ready Computers, Security Technology," *Government Executive Magazine*, 5 October 2001, [http://www.govexec.com/dailyfed/1001/100501h1.htm].

[70]Joshua Dean, "Looking for Lifelines," *Government Executive Magazine*, 1 October 2001, [http://www.govexec.com/features/1001/1001spec4.htm].

[71]Dean, Joshua, "E-gov Fails, Succeeds in Tragedy's Wake," *Government Executive Magazine*, 13 September 2001, [http://www.govexec.com/dailyfed/0901/091301j2.htm].

FEMA regularly updated its Web site with information. The number of visitors to the FEMA site demonstrates the expectations of citizens to be able to find information online. FEMA normally has 500,000 visitors to its site every day. On September 11, 2001, that number soared to 2.3 million. FirstGov was a bit slower in responding, but, by late in the day of September 12, had cobbled together a page providing links to information from a variety of federal, state, and local agencies, as well as non-governmental organizations helping with the crisis. The FBI established a special site to collect tips about the terrorists. Of the 80,000 tips reportedly received within the first five days of the attack, more than half, or 47,052, were received via the Web site.[72] Following the anthrax incidents, the Centers for Disease Control Web site also experienced a notable increase in visitors.[73]

Lessons Regarding Redundancy and Planning of Communications

The third category of lessons learned involves the institutionalization of redundancy in information infrastructures. Redundancy, as used here, includes having computer or network system components, including hardware, software, and telecommunications links, installed and ready to use as a backup in the event primary resources fail. A related aspect of redundancy is the ability to replace and/or reconstruct hardware and software quickly and easily when necessary to prevent extended periods of downtime.

Employment of Redundant Service Providers

Redundancy, or the lack thereof, proved to be critical to many agencies and businesses in lower Manhattan. As described earlier, most of the area's telecommunications lines were connected through two primary switching stations, one of which was destroyed and the other rendered useless due to a lack of electricity. Some organizations that thought they had redundant connections by contracting with two different service providers discovered that both providers used the same central switching office, leaving the organization without service. Approximately 40 of the competitive local exchange carriers in the area relied on Verizon's 140 West Street facility to provide their services.[74]

One group of businesses that did not lose access to their data networks were the tenants of the New York Information Technology Center, an office building located at 55 Broad Street in Manhattan, six blocks from the World Trade Center. Among the services provided by the building's management company is a full telecommunications infrastructure served by 14 voice and data carriers. As a result,

---

[72]Joshua Dean, "Looking for Lifelines," *Government Executive Magazine*, 1 October 2001, [http://www.govexec.com/features/1001/1001spec4.htm].

[73]Joshua Dean, "Federal Web Sites See Spike in Traffic," *Government Executive Magazine*, 26 October 2001, [http://www.govexec.com/dailyfed/1001/102601j1.htm].

[74]Alorie Gilbert, "Out of the Ashes," *InformationWeek*, 7 January 2002, [http://www.informationweek.com/story/IWK20020104S0008].

it was reported that none of the tenants lost access to their data networks, and the few tenants who did use Verizon's voice services were able to switch to another of the building's providers within 24 hours.[75]

Two other companies that had redundant networks were Lehman Brothers and Empire Blue Cross Blue Shield. Lehman Brothers, which had offices both in and around the World Trade Center, had fully redundant networks in Manhattan and in Jersey City, NJ, along with duplicative wide-area links that kept all 45 of its branches connected.[76] Empire Blue Cross Blue Shield, whose backup system was referred to earlier, also had multiple voice and data carriers that connected its World Trade Center offices to its redundant data centers outside of Manhattan, which allowed the insurance carrier to continue to serve its 4.5 million customers.[77] Once its new building in Brooklyn is completed, the insurance carrier plans to install satellite receivers on the roof so it can transmit data between facilities worldwide. In addition to being a less expensive alternative to using several high speed land lines, the satellite receivers will also enable the company to continue to transmit data in the event that the city's land line infrastructure experiences a disruption.[78]

Use of Generic Replaceable Technology

A related lesson that some organizations have cited as valuable to their ability to rebuild their systems quickly is the use of generic, replaceable technology. Agencies and financial firms faced with the need to rebuild their systems quickly -– in some cases, in a matter of days –- received a significant amount of support from many of the major technology vendors, including, but not limited to, Compaq, Dell, IBM, and Sun Microsystems. Drawing from their existing stock of equipment, and ramping up production, the vendors were able to supply large amounts of equipment on short notice. Several information technology companies donated equipment and services to federal agencies in Virginia and New York to assist with recovery efforts.[79] Many vendors also provided discounts, sometimes as high as 80%, for their commercial clients.[80] Vendor support also came in the form of emergency help desk support, cross-country equipment deliveries, and on-site technical support. For example, IBM helped Empire Blue Cross Blue Shield replace over 2,200 desktops

---

[75]Alorie Gilbert, "Out of the Ashes," *InformationWeek*, 7 January 2002, [http://www.informationweek.com/story/IWK20020104S0008].

[76]Sharon Gaudin, "Lehman Brothers Network Survives," *Network World*, 26 November 2001, [http://www.nwfusion.com/research/2001/1126feat.html].

[77]Alorie Gilbert, "Out of the Ashes," *InformationWeek*, 7 January 2002, [http://www.informationweek.com/story/IWK20020104S0008].

[78]Larry Greenemeier, "Empire Blue Cross Soon to Post 'Just Moved' Signs," *InformationWeek*, 6 May 2002, p. 85.

[79]Kellie Lunney, "Federal Contractors Lend Services to Relief Efforts," *Government Executive Magazine*, 20 September 2001, [http://www.govexec.com/dailyfed/0901/092001m1.htm].

[80]Brian Ploskina, "Company Gets Back Up With Help," *Interactive Week*, 1 October 2001, p.19.

and 413 laptops, while Compaq replaced the insurance carrier's 256 servers.[81] Dell and Compaq also provided the American Red Cross with desktops, laptops, servers, and other equipment to assist with the relief efforts.[82] Based on the experience of September 11, 2001, the ability to replace equipment quickly with easy-to-find products that do not require significant customization is likely to be one of the factors affecting organizations' future continuity and disaster recovery planning decisions.

Future Considerations

Although there are undoubtedly additional lessons learned from the September 11, 2001 attacks, the lessons highlighted in the previous pages provide a broad sense of the breadth and depth of the issues facing public and private sector organizations. While not all-inclusive, they emphasize three general approaches: the establishment and practice of comprehensive continuity and recovery plans, the decentralization of operations, and the development of system redundancies to eliminate single points of weakness. The lessons learned from September 11, 2001 build, in part, upon the lessons learned from the 1993 World Trade Center bombing and the preparation for the Y2k transition. However, as agencies and businesses move ahead with continuity planning and implementation, there are indicators that the character of this preparation is changing.

Emphasis on Business Continuity Over Disaster Recovery

One change is that the new lessons learned appear to represent the shift to a higher standard of continuity and disaster recovery planning.[83] Comprehensive contingency plans, perhaps once viewed, at the least, as optional and, at the most, as a prudent measure, may now be seen as an integral part of developing and maintaining an organization's information technology infrastructure. Once

---

[81]Bob Brewin Matt Hamblen, "Alternative Nets Essential in Dealing with Disaster," *Computerworld*, 24 September 2001, p.69.

[82]Compaq Computer Corporation, "Compaq Provides Technology to American Red Cross, Donates to United Way September 11 Fund to Aid New York, D.C. Disaster-Relief Efforts," Press statement, 17 September 2001, [http://www.compaq.com/newsroom/pr/2001/pr2001091704.html]; Dell Computer Corporation, "Dell, Company Employees Anticipate $3 Million Contribution to New York, Washington Relief Efforts," Press statement, 18 September 2001, [http://www.dell.com/us/en/gen/corporate/press/pressoffice_us_2001-09-18-aus-001.htm].

[83]The terms 'disaster recovery' and 'business continuity' are often used interchangeably with little agreement as to their differences. However, disaster recovery is more of a reactive function and is usually used in the context of an organization's ability to respond to a specific event. This involves rebuilding and reconstituting capabilities damaged by a natural or manmade disaster and could include having a period of downtime in which services cannot be delivered. Business continuity, on the other hand, is more of a proactive function in which an organization ensures its ability to continue to operate, perhaps at a reduced capacity and for an extended period of time until normal facilities are restored, with little or no interruption of service in the event of a disaster. Business continuity also usually includes a wider range of logistical concerns beyond technology, such as employee communications, alternative office locations, and client interactions.

considered a remote possibility, the permanent loss of a facility, while still unlikely, must now be taken more seriously. Consequently, an increasing number of organizations, including small and mid-sized companies who often have more limited resources, have begun to focus not just on disaster recovery, but on business continuity. In a networked economy, the costs of network downtime can be measured in tens of thousands of dollars per hour, and as high as one million dollars per hour for highly technology-dependent entities such as infrastructure services firms and energy companies.[84] Other concerns, such as the loss of electricity, the increased frequency of computer viruses, and high-profile hacking attempts have also spurred many organizations to focus on comprehensive business continuity planning rather than disaster recovery alone.[85]

In addition to these higher standards, there is also greater recognition of the qualitative change in preparation. Whereas some organizations may have felt their Y2k readiness measures provided adequate protection, there is now a greater realization that continuity and disaster recovery planning is an open-ended and evolving process, requiring reinforced and redundant infrastructures, regular practice exercises, and testing of data backups and systems. For example, the Pentagon, which already had contingency plans in place, has since embarked on its Command Communications Survivability Project in an effort to redesign its information technology contingency plans.[86] In Congress, Senator Ted Stevens introduced an amendment (SA 2450) to the Department of Defense Appropriations Act, 2002 (P.L. 107-117) on December 7, 2001 that would have required agencies to have "redundant and physically separate" telecommunications systems in an attempt to maintain the operability of communications of government offices in the event of an attack or catastrophe. The amendment passed on a voice vote in the Senate but did not pass in the House of Representatives.[87]

Information Sharing and Collaboration

Another change is the potential for increased information sharing between federal, state, and local government, as well as between the public and private sectors. While information sharing figures prominently in plans for law enforcement-related homeland security activities, it also may play an important role in continuity planning and critical information infrastructure protection. For example, the Chief Information Officers (CIO) Council, which serves as an interagency forum for the CIOs of thirty federal departments and agencies, decided to include a representative from the National Association of State Chief Information

---

[84]James M. Gifford, "Companies Slow to Enact IT Protection Plans," *Federal Times*, Homeland Security & Information Technology Supplement, 10 June 2002, p. 6; James M. Gifford, "Disaster Recovery Technology Moves Off the Back Burner," *Federal Times*, Homeland Security & Information Technology Supplement, 6 June 2002, p. 6.

[85]Jennifer Jones, "Rethinking Plan B," *Federal Computer Week*, 29 April 2002, p. 18.

[86]Christopher J. Dorobek, "DOD Preps Virtual Pentagon," *Federal Computer Week*, 12 August 2002, p. 10; Christopher J. Dorobek, "DOD Reinforces 'Virtual Pentagon'," *Federal Computer Week*, 29 April 2002, p. 19.

[87]"Federal Phones Vulnerable, Industry Says," *Federal Times*, 5 August 2002, p. 4.

Officers (NASCIO) in its activities. In addition to collaborating on issues such as interoperability in wireless communications and electronic government initiatives, several state CIOs are working with the Office of Homeland Security on efforts to protect against terrorism.[88]

Another example is Operation Dark Screen, initiated by Representative Ciro Rodriguez.[89] The three-phase exercise will be conducted over several months during 2002 and 2003 as a partnership between federal, state, and local government, and the private sector. It is designed to test the partners' preparedness to protect critical infrastructures from cyberattacks. There are plans to conduct both a tabletop and a live exercise, as well as an opportunity to implement new protections based on the outcomes of the exercises. As activities such as Operation Dark Screen are carried out, and organizations continue to rebuild and reinforce their information technology assets, it is anticipated that further lessons learned will be added, providing a fuller assessment of our state of readiness, and guidance for the development of future homeland security initiatives.

For Further Reading

CRS Reports

CRS Report RL31594, *Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges*, by R. Eric Petersen and Jeffrey W. Seifert.

CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

CRS Report RL31534, *Critical Infrastructures Remote Control Systems and the Terrorist Threat*, by Dana A. Shea.

CRS Terrorism Electronic Briefing Book EBTER129, *Information and Telecommunications Infrastructure*, by John D. Moteff and Jeffrey W. Seifert.

CRS Report RL31493, *Homeland Security: Department Organization and Management*, by Harold C. Relyea.

CRS Report RL31513, *Homeland Security: Side-by-Side Comparison of H.R. 5005 and S. 2452, 107th Congress*, by the CRS Homeland Security Team.

CRS Report RL31465, *Protecting Critical Infrastructure from Attack: A Catalog of Selected Federal Assistance Programs*, coordinated by John D. Moteff.

---

[88]Dibya Sarkar, "Officials Nurture Relationship," *Federal Computer Week*, 15 July 2002, p. 42.

[89]Dan Caterinicchia, "Cyberterror Test Checks Connections," *Federal Computer Week*, 15 July 2002, [http://www.fcw.com/geb/articles/2002/0715/web-dark-07-15-02.asp].

Other Resources

Dorobek, Christopher J., "Web Sites that Worked," *Federal Computer Week*, 1 October 2001, p.18.

INPUT, *Attack on America: The Impact of the September 11 Terrorist Attacks on the Federal Government*, 3 October 2001, [http://www.input.com/article_printver.cfm?article_id=310].

National Research Council. 2002. *The Internet Under Crisis Conditions: Learning from September 11*. Washington, DC: National Academy Press.

Pentagon Renovation Program Web Site [http://renovation.pentagon.mil/].

Schulz, James, "New Urgency for Disaster Recovery Planning," *Washington Technology*, 8 October 2001, p.18.

"Special Coverage: Attack on America," *Computerworld*, [http://www.computerworld.com/news/special/pages/0,10911,1446,00.html].

"Special Report: September 11, 2001," *Government Executive Magazine*, [http://www.govexec.com/091101report.htm].